

1 DECEMBER 1997



Communications and Information

COMPUTER SYSTEMS MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: <http://afpubs.hq.af.mil>. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/SYND (Mr. James Maloney)
Supersedes AFI 33-112, 6 May 1994.

Certified by: HQ USAF/SCXX (Lt Col Webb)
Pages: 34
Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directives (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*; 33-2, *Information Protection*; and 10-6, *Mission Needs and Operational Requirements*, by identifying responsibilities for supporting Air Force information technology equipment (computer systems). One or more paragraphs of this AFI do not apply to non-Air Force-managed joint service systems. These paragraphs are marked as follows: (*NOT APPLICABLE TO NON-AIR FORCE-MANAGED JOINT SERVICE SYSTEMS*). Selected paragraphs of this publication do not apply to Air National Guard (ANG) units and members. These paragraphs are marked as follows: (*DOES NOT APPLY TO ANG*). Refer technical questions about this AFI to Headquarters Air Force Communications Agency (HQ AFCA/SYND), 203 West Losey Street, Room 3065, Scott AFB IL 62225-5234. Submit policy and procedural recommendations to computer systems management processes to HQ AFCA/SYND. Refer recommended changes and other conflicts between this and other publications to HQ AFCA/XPPX, 203 West Losey Street, Room 1060, Scott AFB IL 62225-5233, on Air Force Form 847, **Recommendation for Change of Publication**. Send an information copy to Headquarters United States Air Force (HQ USAF/SCXX), 1030 Air Force Pentagon, Washington DC 20330-1030. See **Attachment 1** for a glossary of references, abbreviations, acronyms, and terms used in this publication. **Attachment 2** contains an address listing of key organizations.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

This revision supersedes AFI 33-112 dated 6 May 1994, changing the title from “Automatic Data Processing Equipment (ADPE) Management” to “Computer Systems Management.” It improves the flow and organization of material presented; updates organizational changes; defines and clarifies the various roles and responsibilities located throughout the instruction; and incorporates those recommendations identified in the HQ AFCA Functional Process Improvement (FPI) Study, *Air Force ADPE Life-Cycle Management*, dated 15 June 1995. It also narrows the scope of the AFI to the management of computer systems and associated equipment, while referring network and software management to the appropriate

Air Force instructions. It establishes a \$500 floor for most items in the Information Processing Management System (IPMS). It charters the Computer System Management Working Group (CSMWG). It rescinds recurring reporting requirements for HAF-SCP(BA)8901, *Computers and Automatic Data Processing Equipment (ADPE) Management*; HAF-SCM(Q)7104, *Automated Data Processing Equipment (ADPE) Inventory Report*; Interagency Report Control Number (IRC�)-0312-GSA-QU, *Automatic Data Processing Equipment Data System*, and IRC� 1106-GSA-AN, *Annual Report of ADP Services Provided to Another Agency or Obtained from a Commercial Source*. The (I) preceding the publication title indicates a major revision from the previous edition.

Section A	Responsibilities	3
1.	Headquarters United States Air Force, Communications and Information	3
2.	Headquarters United States Air Force, Installation and Logistics	3
3.	Headquarters Air Force Communications and Information Center	3
4.	Headquarters Air Education and Training Command	4
5.	Headquarters Standard Systems Group	4
6.	Communications and Information Systems Officer (CSO)	4
7.	Organization Commanders (or Directors of Special Staff Offices)	5
8.	Organization Computer Manager	6
9.	Major Command Equipment Control Officers	7
10.	Base/Tenant Equipment Control Officer	8
11.	Equipment Custodians	9
12.	Systems Administrator (SA)	10
Section B	General Guidance and Procedures	11
13.	Planning	11
14.	Security	11
15.	Air Force Contractors	12
16.	Air Force Infrastructure Support Contracts	12
17.	Deployment Considerations	13
18.	Installation and Relocation of Computer Systems	13
19.	Use of Computer Systems	14
20.	Purchasing Notebook Computers for General Officers (GO) and Senior Executive Service (SES) Executives	15
21.	Environmental Considerations	16
Section C	Inventory, Accountability, Transfer, and Reporting of Computer Systems	16
22.	Inventory Management	16

23.	Establishing and Closing a Defense Reporting Activity Account	16
24.	Identification of Computer Systems	17
25.	On-Line Computer Systems Inventory	17
26.	Transferring Non-Excess Computer Systems Assets to Another Department of Defense Component, Federal Agency, State, or Local Government	18
Section D	Computer System Maintenance	19
27.	General Information	19
28.	Emission Security-Certified Maintenance	20
29.	Computer Systems Maintenance Reporting	21
30.	Contractor or Air Force Liaison	21
31.	Contractual Matters	21
32.	Computation of Payments	21
Section E	Disposition of Excess Resources	22
33.	Excess Hardware	22
34.	Obtaining Excess Resources	23
35.	Shipping and Disposition of Excess Computer Systems Resources	23
36.	General Ledger Subsidiary Account-16104	23
37.	Checklists	23
38.	Forms Prescribed	24
Attachment 1	GLOSSARY OF REFERENCES, ACRONYMS, ABBREVIATIONS, AND TERMS	25
Attachment 2	KEY ORGANIZATIONS	31
Attachment 3	QUESTIONS FOR COMPUTER SYSTEMS CHECKLIST	34

Section A—Responsibilities

1. Headquarters United States Air Force, Communications and Information (HQ USAF/SC):

- 1.1. Provides regulatory and policy guidance on computer systems (HQ USAF/SCX).
- 1.2. Provides computer systems training oversight (HQ USAF/SCX).

2. Headquarters United States Air Force, Installation and Logistics (HQ USAF/ILM). Approves or disapproves hardware maintenance below the line replaceable unit (LRU) level.

3. Headquarters Air Force Communications and Information Center (HQ AF C IC). A direct reporting unit of HQ USAF/SC:

- 3.1. Resolves operational issues on computer systems (HQ AFCIC/SYS).
- 3.2. Acts as the functional manager for IPMS and the Air Force Computer Systems Redistribution Program (HQ AFCIC/SYS).
- 3.3. Reviews policy and procedural recommendations to computer systems management processes (HQ AFCIC/SYS).
- 3.4. Ensures appropriate action is taken upon receipt of excess equipment requests.
- 3.5. Establishes a new defense reporting activity account (DRA) upon request of the major command equipment control officer (MECO) and receipt of appropriate information.
- 3.6. Reviews concerns expressed by MECOs about inclusion and, or exclusion of computer systems in IPMS.
- 3.7. Includes DRA information received from MECOs and adds to automation resources management system (ARMS) data base.
- 3.8. Serves as Air Force focal point to Defense Information Systems Agency (DISA) concerning questions and, or comments pertaining to Assistant Secretary of Defense (ASD) Memorandum dated September 8, 1994, Subject: *Interim Management Guidance on Defense Automation Resources Management; and Defense Automation Resource Management Manual*, September 1988.
- 3.9. Establish an Air Force CSMWG to support computer systems management (CSM) personnel at all levels in the execution of their responsibilities as outlined in this instruction and other CSM-related guidance.
 - 3.9.1. The CSMWG will include broad representation of CSM functions allowing for improved crossfeed of information and feedback from the field necessary to make informed decisions about CSM policy and procedures.
 - 3.9.2. The CSMWG will:
 - 3.9.2.1. Assist HQ AFCIC/SY to resolve current or anticipated CSM-related issues whether technical, managerial, or administrative.
 - 3.9.2.2. Assist HQ AFCIC/SY to take functional improvement opportunity.
 - 3.9.2.3. Serve as the Air Force CSM infrastructure to deal with CSM-related issues.
 - 3.9.2.4. Identify CSM functional requirements and provide configuration control for automated information systems (AIS) dedicated to Air Force CSM.

4. Headquarters Air Education and Training Command (HQ AETC/TT). Provides oversight of Air Force supplemental technical training. Course E3AZR3C051 019, *Automatic Data Processing Equipment (ADPE) Inventory and Management System*, is a two-week supplemental course conducted at Keesler AFB. This course provides formal training for Air Force personnel involved with CSM. To obtain a quota for this course, respective major commands (MAJCOM) must send a request to Second Air Force (2AF/DOP) either on-line using the Air Force Training Management System (AFTMS) or via hard copy message. See Air Force Catalog (AFCAT) 36-2223, *USAF Formal Schools*, for additional information.

5. Headquarters Standard Systems Group (HQ SSG/ENEI):

- 5.1. Provides IPMS operations, programming, and software support.
- 5.2. Specifies the format for contract tables.
- 5.3. Submits General Ledger Subsidiary Account (GLSA) 16104 report to the Defense Finance and Accounting Service (DFAS/LI-ARF).

6. Communications and Information Systems Officer (CSO):

- 6.1. Ensures every effort is made to use sharing and redistribution programs to meet user requirements.
- 6.2. Processes all base-user computer systems orders except those excluded by host-tenant support agreements and joint service programs managed outside the Air Force.
- 6.3. Is the accountable officer for all equipment listed in their assigned IPMS account. Ensures the IPMS inventory is used to provide accountability of all base computer systems resources assigned to that DRA.
 - 6.3.1. Controls equipment custodian (EC) access to IPMS.
 - 6.3.2. Ensures procedures are in place instructing base communications personnel to use the IPMS to notify and document equipment transfers between bases.
- 6.4. Assists in planning for and executing all activities related to the deployment of joint service systems.
- 6.5. Budgets for maintenance of applicable host-base computer systems.
 - 6.5.1. Follows budgeting arrangements established in host-tenant support agreements.
 - 6.5.2. Develops procedures with the resource managers of the host and tenant organizations to de-obligate excess funds for use on Air Force requirements.
- 6.6. Combines maintenance requirements, prepares and submits performance work statements and surveillance plans (AFI 64-108, *Service Contracts*), and serves as the focal point for maintenance of computer systems.
 - 6.6.1. Assists the supporting contracting officer in developing an acquisition strategy for maintenance contracts.
 - 6.6.2. Ensures annual review of maintenance strategies and reports to verify organizations use the most cost-effective options.
 - 6.6.3. Advises base organizations of local maintenance procedures.
- 6.7. Plans for and provides support during contingencies and deployments.
- 6.8. Finds the most economical source for spare parts.
 - 6.8.1. Directs retention of serviceable excess computer systems for maintenance redundancy or operational spares.
- 6.9. Authorizes cannibalization of unserviceable computer systems for spare parts.
- 6.10. Coordinates action to ensure secure, climate controlled, and easily accessible facilities are provided for receiving, storing, and distributing computer systems.

6.11. Coordinates changes to computer systems requirements with the appropriate command or base communications unit.

6.12. Provides the appointment letter of the equipment control officers (ECO).

6.12.1. The MAJCOM CSO appoints the MECO. The MECO will hold a grade of master sergeant (or above), or civilian of equivalent grade. MECO responsibilities do not include equipment accountability.

6.13. Ensures mandatory training is provided within 45 days before an individual assumes duty as an ECO or has previous experience as an ECO.

6.14. Collects small computer maintenance cost data needed to evaluate maintenance methods to obtain the most cost-effective maintenance.

7. Organization Commanders (or Directors of Special Staff Offices). Each commander or director of special staff office with computer system resources establishes policies and procedures for management and support of the organization's computer systems resources. The commander is responsible for all computer systems assigned to their unit.

7.1. Budgets for maintenance of computer systems that are not the responsibility of the CSO.

7.2. Reviews and coordinates on organization's requirement documents.

7.3. Submits unit computer systems requirements to the applicable CSO for technical solutions according to AFI 33-103, *Requirements Development and Processing*.

7.4. Reviews their systems annually to determine if the systems still meet user requirements, need modification, or are obsolete.

7.5. Designates, in writing, a minimum of one EC and alternate, depending on span of control.

7.5.1. Appoints a new EC not later than 45 days before the departure of the present EC. Forwards appointment letter and request for EC training to the applicable ECO.

7.5.2. Requires departing EC to process out through the ECO.

7.5.3. Requires outgoing and incoming EC to conduct a joint physical inventory and reconcile missing items under the guidance of the ECO. The new custodian provides the old custodian a signed copy of the IPMS ADPE custodian inventory custodial listing. In cases of a permanent change of station (PCS), the new custodian will initial the clearance record of the outgoing custodian to indicate the custodian's account is clear and that the custodian can comply with PCS orders.

7.5.3.1. Custodians, supervisors, and others directly involved in equipment transfers must ensure custodial record listings are correct and property is accounted for. Failure to comply can result in personnel declared contributory negligent when a report of survey (ROS) is initiated, because they created or condoned conditions or practices that favored the loss or damage of property.

7.6. Annually certifies to the applicable ECO the appointment of the ECs, that the ECs have received the required training, and that an annual physical inventory was accomplished for all computer systems under their jurisdiction. Complete this certification each year, no later than the day each individual was officially appointed a custodian.

- 7.7. Ensures the EC notifies the applicable ECO of any computer systems that are scheduled for deployment.
- 7.8. Promotes user awareness concerning unauthorized or illegal use of computer systems' hardware and software.
- 7.9. Ensures organizations do not use shareware or public domain software until the CSO certifies computer systems are free of viruses, hidden defects, or obvious copyright infringements, and that organization shareware users pay any necessary fees prior to utilization.
- 7.10. Ensures all computer systems assets (including those purchased using the International Merchant Purchase Authorization Card [IMPAC]) are reported to the EC and ECO.
- 7.11. Ensures that the applicable ECO coordinates on the "Ship To" addressee on all purchase requests or transfers that involve computer systems.
- 7.12. Ensures the EC properly receives and secures computer systems until proper accountability procedures are accomplished.
- 7.13. Has the authority to sign for new equipment and may delegate that authority only to their ECs.
- 7.14. Appoints an organization computer manager (OCM).

8. (DOES NOT APPLY TO ANG) Organization Computer Manager. The OCM is appointed by the organization commander. The OCM assists in the performance of the commander's responsibilities and is the focal point for computer operation (not accountability) issues. The OCM:

- 8.1. Sends properly documented requirements to the applicable CSO for action.
- 8.2. Coordinates with the network control center (NCC) in establishing contingency procedures for manual backups, reallocation of computer resources, etc., for systems critical to mission accomplishment.
- 8.3. Coordinates support issues with applicable agencies.
- 8.4. Assists with installing, testing, and accepting the system according to the terms of the purchase contract and instructions.
- 8.5. Coordinates with the facility manager and the base civil engineer for facility support requirements.
- 8.6. Periodically reviews the organization's needs for computer resources. Identifies training needs, manpower issues, etc.
- 8.7. Validates computer systems and equipment requirements submitted by the unit EC.
- 8.8. Works with the NCC to ensure network management procedures comply with contracting documents.
- 8.9. Reports excess computer resources to the organization ADPE EC at least 120 days before the resources are no longer required.
- 8.10. Assists organization commander in planning for support of deployments.
- 8.11. Assists others within their organization to resolve computer systems problems.

8.12. Manages all computer equipment and software, and their interfaces to systems and networks according to this instruction and AFI 33-114, *Software Management*, and AFI 33-115, *Networks Management*.

9. Major Command Equipment Control Officers.

9.1. MECOs:

9.1.1. Oversee all accountable computer systems within the MAJCOM managed by assigned applicable ECO.

9.1.2. Work with other MECOs to determine reporting procedures of tenant units and continue to work together to resolve any problems that might arise.

9.1.3. Have the authority to transfer excess equipment to other MAJCOMs.

9.1.4. Forward applicable ECO concerns about the inclusion and, or exclusion of computer systems in IPMS to HQ AFCIC/SYSS.

9.1.5. Review finalized excess reports completed by applicable ECOs and ensure appropriate action is accomplished.

9.1.6. Promptly process excess requests and forward to HQ AFCIC/SYSS for action when necessary.

9.1.7. Allow ECOs to create and maintain holding accounts for known near-term requirements.

9.1.8. Assist ECOs, when requested, in searching for found-on-base (FOB) computer systems within and outside the command.

9.1.9. Coordinate the creation of a new DRA as needed, and forward all appropriate information to HQ AFCIC/SYSS to establish the new account in the ARMS.

9.1.9.1. Ensure a new applicable ECO is appointed in writing.

9.1.9.2. Ensure a new applicable ECO establishes IPMS connectivity.

9.1.10. Provide assistance to applicable ECOs in closing out a DRA (e.g., base closures).

9.1.11. Allow access by the program management office (PMO) to establish vendor contract and group tables if they meet the established criteria.

9.1.12. Forward any information related to a PMO requirement to all applicable ECOs.

9.1.13. Establish accountability procedures for computer systems acquired through joint services, working with the applicable ECOs and PMO.

9.1.14. Notify the PMO of centrally managed programs of any excess equipment acquired for that program that is available for reutilization.

10. Base/Tenant Equipment Control Officer.

10.1. The CSO appoints the ECO and forwards the appointment letter to the MECO. The ECO will hold a grade of master sergeant or above, or civilian of equivalent grade. The installation commander may approve a one-grade reduction.

10.2. The ECO:

- 10.2.1. Receives all computer systems, ensuring accountability and completion of all necessary documentation.
- 10.2.2. Is accountable for equipment listed in their assigned IPMS account. Ensures accountability of computer systems acquired through any source.
- 10.2.3. Attempts to determine ownership of all FOB computer systems and takes appropriate action to ensure accountability.
- 10.2.4. Updates IPMS and clears errors before the first Sunday of each month as required for upward reporting.
- 10.2.5. Directs all ECs to conduct an annual physical inventory of assigned computer systems. Ensures completion of the annual physical inventory and that EC appointments are renewed annually.
- 10.2.6. Forwards questions concerning the inclusion and, or exclusion of computer systems in IPMS to the MECO.
- 10.2.7. Retains serviceable excess computer systems for maintenance redundancy or operational spares.
- 10.2.8. Retains unserviceable excess computer systems for cannibalization as directed by the CSO.
- 10.2.9. Ensures correct major command code (MAC) utilization for all computer systems in their IPMS DRA.
- 10.2.10. Prepares IPMS bar code (or equivalent) identification labels and provides them to the EC as needed.
- 10.2.11. Takes appropriate action to update the inventory as dictated by a ROS.
- 10.2.12. Completes out-processing for departing EC upon transfer of account and receipt of new appointment letters.
- 10.2.13. Provides guidance and training for the EC.
- 10.2.14. Takes guidance and direction from the MECO.
- 10.2.15. Coordinates the establishment of a new DRA and IPMS connectivity as directed by the MECO.
- 10.2.16. Correctly codes deployed computer systems in IPMS as directed by HQ USAF or MAJCOM and authorized by the applicable CSO.
- 10.2.17. Establishes accountability for computer systems acquired through joint services, working with the parent MAJCOM.
- 10.2.18. Attempts intra-command DRA redistribution of excess computer systems to satisfy local requirements before the completion of any excess reports.
- 10.2.19. Creates electronic excess reports in IPMS for excess equipment items that are not required locally.
- 10.2.20. Searches, when requested or needed, the reuse module in IPMS for available excess computer systems Air Force-wide to satisfy local requirements.

10.2.21. Directs preparation of Department of Defense (DD) Form 1149, **Requisition and Invoice/Shipping Document**, as needed to request excess from other activities or the Defense Reutilization and Marketing Office (DRMO), and forwards through command channels.

10.2.22. Ensures prompt shipment of excess computer systems and associated accountability records as directed by PMO, MECO, HQ AFCIC/SYSS, or DISA.

10.2.22.1. Notifies the MECO of centrally managed programs of any excess equipment acquired for that program that is available for reutilization.

10.2.23. When applicable, processes and maintains AF Form 597, **ADPE Maintenance Record**, or applicable vendor maintenance form.

10.2.24. Notifies applicable maintenance contract office of primary responsibility (OPR) to remove from maintenance computer systems that become excess and are not required for reuse locally.

10.2.25. Works with any tenant ECO to establish a host-tenant agreement identifying any assistance required, such as IPMS connectivity.

10.2.26. Coordinates on all host-tenant agreements.

10.2.27. Executes memorandum of agreement (MOA) between losing and gaining organizations when transferring non-excess computer systems, and forwards a copy of the MOA to the MECO and HQ AFCIC/SYSS.

10.2.28. Coordinates on the MOA for non-Air Force managed joint service systems.

10.2.29. Uses the completed ROS (DD Form 200, **Financial Liability Investigation of Property Loss**) as authority (source document) to update the inventory.

11. Equipment Custodians. ECs and their alternates are appointed by the organizational commander. ECs:

11.1. Are responsible for all assigned computer systems.

11.1.1. The EC will perform an annual physical inventory as directed by the ECO. Upon completion, the inventory is signed by the EC and ECO with the original copy retained by the EC.

11.2. Ensure all accountable computer systems and equipment have a personal computer (PC) IPMS bar code label (or equivalent) attached. Use AF Form 992, **ADPE Identification**, until bar code capability is available.

11.3. Obtain approval and coordinate all potential transfers of computer systems between accounts with the applicable ECO. (**NOTE:** The ECs have no authority to transfer computer systems outside their account.)

11.4. Report all FOB computer systems and pick up accountability or return equipment as directed by the applicable ECO.

11.5. Sign for new equipment as well as all assigned accountable computer systems.

11.6. Ship excess computer systems or turn into DRMO as directed by the applicable ECO.

11.7. Provide appropriate documentation back to the applicable ECO to clear the account of equipment that was transferred to another account, turned-in to the DRMO, or donated to a school.

- 11.8. Remain responsive to applicable ECO.
- 11.9. Must out-process through the applicable ECO.
- 11.10. Conduct a joint physical inventory and reconcile any missing items before the departure of the present EC or as directed by the applicable ECO.
- 11.11. Notify the applicable ECO at least 120 days before computer systems go off-line to allow completion of the screening cycle while the equipment is still in use.
- 11.12. Immediately notify the organizational commander to appoint an investigating official to begin the ROS process for any loss, damage, or destruction of computer systems. Notify and provide a copy of the completed ROS (DD Form 200) to the applicable ECO and security police.
- 11.13. Report excess computer systems accounted for in base supply through base supply.
- 11.14. Notify applicable ECO of any deployed computer systems.
- 11.15. Properly receive and secure computer systems until proper accountability procedures are accomplished.

12. Systems Administrator (SA). The SA manages the resources of the entire computer system. One person may serve as the SA for more than one multiuser system. Selecting a well-qualified SA is critical to a successful multiuser system. The SA works closely with the OCM and NCC workcenter. SAs:

- 12.1. Configure the operating system software to meet user needs (e.g., assigning user profiles, defining printer or modem access, and setting up user restrictions).
- 12.2. Define ownership of applications and determining who has permission to read, write, and execute.
- 12.3. Assign log-ons, passwords, and user privileges on the system (e.g., which users share files).
- 12.4. Plan for short-term and long-term loss of system hardware and software. In configuring the system, the SA and network security manager must decide on contingency plans in case of the SA's absence. This may involve having another SA administer the system through a modem.
- 12.5. Perform routine system maintenance, such as backing up or archiving files and adding software updates.
- 12.6. Contact the OCM or NCC for hardware maintenance.
- 12.7. Work with the network security manager to set up network security policies and procedures. The SA monitors system security and change passwords periodically. Refer to Air Force systems security instruction (AFSSI) and manual (AFSSM) 5000-series publications, and Air Force Index (AFIND) 5, *Numerical Index of Specialized Information Protection Publications*, for further guidance.
- 12.8. Train users, when possible.
- 12.9. Provide user manuals that include sign-on and sign-off procedures, use of basic commands, software policies, user responsibilities, etc.

Section B—General Guidance and Procedures

13. Planning. The OCM must review AFI 33-102, *Command, Control, Communications, Computers, and Intelligence (C4I) Capabilities Planning Process*; AFI 33-103; and AFI 33-104, *Base-Level Planning and Implementation*, before defining requirements and planning for new computer systems.

13.1. Consider support requirements for operations, deployments, contingencies and exercises, access for handicapped personnel, security, information sharing with other resources, management of records, and environmental considerations before purchasing computer systems or associated equipment.

13.2. Closely monitor the acquisition process to ensure required support is in place before receipt of the equipment or systems. Using organizations are responsible for the use, management, and maintenance of required computer systems and associated equipment.

13.3. Contact your wing information protection (IP) office before initiating procurement action. They will advise planners on the security aspects and verify the equipment meets emission security (EMSEC) and other requirements are included.

14. Security. Using organizations are responsible for the development of policies and procedures to protect computer system resources under their control. For specialized information refer to those documents listed in **Attachment 1**, and applicable AFSSIs and AFSSMs listed in AFIND 5.

14.1. Obtain written approval from the local designated approving authority (DAA) prior to the use or connection of new computer system resources.

14.2. Obtain special certification and guidance before ordering, installing, and using computer system resources (hardware and software) for use within Sensitive Compartmented Information Facility (SCIF) areas.

14.3. Computer systems accreditation is tracked in the IPMS. System managers and the supporting IP office will ensure that systems accreditation is entered in the IPMS.

15. Air Force Contractors. Obtain the approval of your local DAA before allowing a contractor access to, or operation of, government-furnished or contractor-owned computer system resources processing government information. The local procurement office can provide guidance on providing government-furnished computer system resources for contractor use (see AFI 31-601, *Industrial Security Program Management*, and Department of Defense Manual [DODM] 5200.28, *ADP Security Manual*, January 1973, with Change 1).

15.1. Contractors may function as a custodian or as an accountable officer as the contract specifies. Establish the extent of contractor liability in the provisions of the applicable contract's government property clause (see AFI 23-111, *Management of Government Property in Possession of the Air Force*).

16. Air Force Infrastructure Support Contracts. These contracts provide computer system resources at discount prices, offer a standard structure for Air Force-wide maintenance and training, and simplify integration and interoperability of computer systems. These contracts include Desk Top IV, V, ULANA I & II, etc.

16.1. The CSO will utilize Air Force infrastructure support contracts (when such contracts meet mission requirements) for obtaining all Air Force computer system needs, including local area network (LAN) acquisitions. Some of these contracts may contain mandatory purchase items. Direct questions about infrastructure support contracts to HQ SSG/SSMC.

16.2. The contractor will provide necessary tables to the government for inventory record creation, data validation, and order processing.

16.3. IPMS Ordering Module:

16.3.1. All centralized PMOs that order computer systems or equipment from a standard Air Force infrastructure contract for multiple MAJCOMs must enter and maintain vendor contract, cost, and group tables in IPMS as specified by HQ SSG/ENEI. Make sure these tables, and all subsequent updates, are available in IPMS before the effective date of the initial release or update. Additionally, process all orders for computer systems or equipment from a standard Air Force infrastructure contract through an ordering module in IPMS. Provide funding support for maintaining these tables and the ordering module to HQ SSG/ENEI by the contract PMO. Provide HQ SSG/ENEI sufficient lead time for implementation of the ordering module before the effective date of the contract or update. This ordering module must provide the functionality specified by HQ SSG/ENEI. This functionality, with the other IPMS modules, must, at a minimum, provide:

16.3.1.1. Automatic creation, addition, and, or modification of inventory records to the gaining organization's IPMS data base when specific contract orders are processed.

16.3.1.2. Validation of inventory record data field in the IPMS data base.

16.3.1.3. Standardized inventory record data entry.

16.3.1.4. Reliable inventory tracking and life-cycle management of computer systems and equipment processed through IPMS.

16.3.1.5. Oversight of funding and computer system/equipment redistribution requirements.

16.4. (*DOES NOT APPLY TO ANG*) All MAJCOM centralized PMOs ordering computer systems from their own unique contracts (with a total annual funding of \$2 million or more in any one year, or \$25 million or more over the program life cycle) must comply with the vendor contract, cost, and group table requirements, plus the ordering module requirements, outlined in paragraph 16.3.1.

16.4.1. MAJCOMs managing the contract must provide funding to HQ SSG/ENEI. PMOs can access IPMS for this input by going through either their MECO or MAJCOM IPMS coordinator. Use MAJCOM-unique contract tables for MAJCOM non-standard contracts just as you use standard contract tables for Air Force standard contracts.

17. Deployment Considerations. The MAJCOM CSO must address support and security guidance requirements for the deployment of computer systems within their command.

17.1. This guidance must include:

17.1.1. The packing, shipping, installing, operating, and maintaining of computer systems in the deployed location.

17.1.2. Planning for requirements needed to provide support to deployed resources (i.e., connectivity to LANs, Defense Data Network [DDN], Non-Classified Internet Protocol Network [NIPR-NET], etc.).

17.1.3. Support agreements (such as inter-service or host-nation).

17.1.4. Facility support.

17.1.5. Security issues.

17.1.6. Logistics support.

17.1.7. The establishment of a MOA addressing responsibilities for support of joint systems, whether managed by an Air Force program office or by another Department of Defense (DoD) element.

17.1.8. The movement of primary and backup resources on different vehicles or aircraft.

17.2. The ECO will use a one-position deployment asset field (data field "I" in the IPMS) to identify computer systems authorized for deployment.

17.3. The CSO submits a requirement, with justification, to the associated unit type code (UTC) pilot unit when plans involve deploying computer systems as part of a specific UTC on a long-term, continuing basis. The UTC pilot unit updates the UTC mission capability statement and equipment list to ensure the appropriate logistical support for the deployed (gained) equipment. This support may include spare parts or the proper readiness spares package inventory to support the new equipment.

18. Installation and Relocation of Computer Systems.

18.1. Installation:

18.1.1. The CSO is responsible for determining whether the using organization, communications unit, or outside agency will install the equipment or software.

18.1.2. Using organizations are normally responsible for installing stand-alone small computers, peripherals, and software. When installing computer systems:

18.1.2.1. Follow installation procedures and checklists established by the vendor contract, MAJCOM, CSO, and OCM.

18.1.2.2. Ensure all pre-installation requirements are completed before installation of computer systems.

18.1.2.3. Contact your communications unit plans flight office and OCM before beginning installation.

18.1.2.4. Contact the NCC workcenter for needed assistance.

18.1.3. The installation of EMSEC. EMSEC-certified required systems may differ from that of non-EMSEC-certified systems.

18.1.4. Responsibility for testing the equipment and identifying hardware or software problems lies with the using organization. When appropriate, correct problems or defects under the manufacturer's warranty.

18.1.5. Using organizations must ensure contractors complete all contract requirements and any implementation checklists provided by the CSO.

18.2. Relocation:

18.2.1. Do not relocate accountable computer systems without first notifying the EC.

18.2.2. Notify the responsible EC before removing equipment from the EC account.

18.2.3. Installation of relocated computer systems and software is the responsibility of the using organization.

18.2.4. The vender or CSO may install or relocate large or complex systems.

19. Use of Computer Systems.

19.1. Use computer systems for official or authorized purposes only. Commanders may authorize use of government resources for personal projects if they determine the use is in the best interest of the Air Force; document the authorization in organizational policy or by letter to the individual concerned. Commanders and supervisors may authorize any use allowed by the Uniform Code of Military Justice (UCMJ) and Joint Ethics Regulation, and does not interfere with mission performance.

19.2. Do not use privately owned computer systems to:

19.2.1. Automate functions in support of the unit's mission.

19.2.2. Process classified or Privacy Act data.

19.3. Data entered on privately owned computer systems or software developed while performing government business becomes the property of the U.S. Government.

19.4. The government will not incur any cost or liability resulting from the use, misuse, loss, theft, or destruction of privately owned computer systems resources.

19.5. Alternate Work Locations. Unit commanders, in coordination with the local personnel office, may authorize personnel to work at an alternate work location (including the employee's home). Unit commanders may also authorize installation of a PC, applicable software, modems, fax machines, and data (telephone) lines to support access at the alternate work location (see Federal Personnel Manual System, FPM Letter 368-1 dated 26 March 1991, Subject: *Federal Flexible Workplace Project*; and Public Law 104-52, *Telephone Installation and Charges*, page 109 STAT 468, Section 620 [31 U.S.C. 1348]. Commanders must consider the cost of providing necessary communications and computer systems services before allowing personnel to work from an alternate work location.

19.5.1. The unit commander authorizing the alternate work location must:

19.5.1.1. Determine the service is necessary for direct support of the agency's mission.

19.5.1.2. Fund for necessary equipment, software, LAN access, and phone lines necessary to support the mission.

19.5.1.3. Make sure the alternate work location is an economical option to having the individual work in the office.

19.5.1.4. Authorize payment for installation and monthly recurring charges.

19.5.1.5. Certify that adequate monitoring capabilities and safeguards against private misuse

exist.

19.5.1.6. Account for equipment on a hand receipt and inventory annually.

19.5.1.7. Notify the ECO of the relocation of the equipment.

19.5.2. The individual authorized an alternate work location is responsible for providing adequate security against equipment and software loss, theft or damage (physical and virus), or misuse. The individual is also responsible for ensuring use of government equipment and government-provided services at the alternate work location are for official use only.

20. (DOES NOT APPLY TO ANG) Purchasing Notebook Computers for General Officers (GO) and Senior Executive Service (SES) Executives.

20.1. The purchasing of notebook computers as professional equipment for new GOs and senior executives (SE) was approved in March 1995. The notebook computer will accompany the GO or SE from assignment to assignment. The Air Force General Officer Matters Office (AFGOMO) normally funds and procures notebooks for new GOs and accounts for them under a central DRA maintained by the Air Force Pentagon Communications Agency (AFPCA/LASA). In cases where a local communications unit buys the computer systems as a maintenance replacement or technology upgrade, they will forward appropriate equipment control information pertaining to the new notebook computer to AFGOMO. The local communications unit will forward appropriate information pertaining to the new notebook computer to DRA 3500, AFPCA/LASA. The local DRA manager will account for the notebook currently issued to a senior leader until the GO or SE PCSs. At that time, the local communications unit will transfer the notebook records to AFGOMO who will maintain applicable warranty information in the central account.

20.1.1. The local communications unit is responsible for technology refreshment and hardware maintenance.

20.1.2. When a GO or SE retires or leaves Air Force service, the GO or SE must turn in the notebook computer to the local Air Force CSO. Individuals not assigned to Air Force bases may turn them in to the nearest Air Force CSO or return them to AFGOMO. The CSO receiving the notebook computers should contact AFGOMO to initiate a transfer of the notebook computer to the local equipment account.

20.1.3. AFPCA/LASA will, upon receipt of the equipment control information, generate PC-IPMS bar code label and send it to the GO or SE via their executive officer or local CSO, as appropriate.

21. Environmental Considerations. Use hardware and software within the environmental parameters defined by the vendor (e.g., power, temperature, humidity, etc.).

21.1. Equipment damage outside these parameters may void the warranty or incur an added cost liability according to the contract constraints.

21.2. Commanders may authorize use outside the environmental parameters if mission requirements dictate (e.g., as in deployed operations).

Section C—Inventory, Accountability, Transfer, and Reporting of Computer Systems

22. Inventory Management. A threshold of \$500 is established for mandatory inclusion of items in the IPMS.

22.1. You are not required to enter (record) items costing less than \$500 or with a current market value of less than \$500 into the IPMS except for the following:

22.1.1. Main central processing unit (CPU) of each system for registering computer system security accreditation regardless of value.

22.1.2. Equipment turned in for reuse screening.

22.2. Commanders, managers, and individuals must maintain and protect all items assigned to them. Commanders at any level may require the inclusion of additional items in the appropriate level IPMS inventory. Coordinate additions through the supporting communications unit.

22.3. Internal components and dedicated peripherals (e.g., mouse, keyboard) purchased with the CPU, or costing less than \$500, do not require separate tracking; consider including these items as features of the CPU.

23. Establishing and Closing a Defense Reporting Activity Account.

23.1. The MECO may direct the creation of a DRA.

23.1.1. The requesting organization contacts the MECO to establish a DRA and provides the information required by applicable DoD directives. See ASD Memorandum dated September 8, 1994, Subject: *Interim Management Guidance on Defense Automation Resource Management for additional information.*

23.1.2. The MECO forwards information about the DRA to HQ AFCIC/SYSS for addition to the ARMS data base. MAJCOMs have approval authority for DRA management.

23.1.3. The MECO establishes the DRA number in IPMS.

23.1.4. The MECO contacts the new ECO to verify IPMS connection.

23.2. When their units are tenants on another MAJCOM's base, the parent MECO will work with the host MECO to determine reporting procedures (e.g., resolving inventory discrepancies).

23.3. Host-tenant support agreements must state whether tenants report their computer systems under the 4-digit data DRA number of the host-base or under a DRA number assigned by their parent MAJCOM.

23.4. To close a DRA:

23.4.1. ECOs close all records and inform the MECO of the closure.

23.4.2. The MECO will contact the HQ SSG/ENEI program office to formally close the DRA.

23.4.3. The MECO will inform HQ AFCIC/SYSS that the DRA is closed and that all computer systems and equipment were properly disposed of or transferred to another DRA.

23.4.4. Indicate that the data was shipped in IPMS.

24. Identification of Computer Systems.

24.1. The ECO will use PC-IPMS bar code labels, if available. Otherwise, prepare AF Form 992. If AF Form 992 is not available, use electronically generated computer systems/equipment labels. Make sure the labels are plain, white, and self-adhesive.

24.2. The EC will attach a current AF Form 992, bar code label or equivalent to each accountable computer system item in their activity to expedite proper identification, inventory, maintenance, and reporting of computer systems.

24.3. FOB (Small Computers and Equipment). Immediately report any computer or equipment items that are FOB to the applicable ECO. The ECO will use the IPMS to determine equipment ownership. If the ECO cannot determine ownership, the ECO will take action to ensure proper accountability.

24.3.1. Computer systems FOB without a bar code label or computer equipment/system label attached. Forward applicable data to the MECO who will initiate a search of the IPMS and temporarily enter the item into the finding organizations account pending results of this search.

24.3.2. If the search fails to identify ownership, the finding EC will attempt to use the item to satisfy a validated requirement. If the EC cannot use the equipment to satisfy an existing or future requirement, declare the equipment excess and take appropriate action.

25. On-Line Computer Systems Inventory.

25.1. The on-line Air Force IPMS is the official Air Force system for the accountability, tracking, and reporting of computer systems.

25.1.1. Upon receipt of a DD Form 1155, **Order for Supplies or Services**, or other purchasing document, the ECO will enter applicable data into the IPMS and establish a suspense system. All activity ECOs process updates as they occur and enter applicable data into their computer systems inventory through the on-line IPMS. ECOs transmit on-line inventory updates through Defense Information Systems Network (DISN) to the IPMS data base at Maxwell AFB-Gunter Annex. This report is designated emergency status code C-3 (continue reporting during emergency conditions, delayed) and submit data requirements as prescribed. You may delay these reports to allow the submission of higher precedence reports.

25.1.2. Identify assets reported by the host-base for a tenant organization by the 2-position MAC (data element name is MAC) listed in the MAC table in IPMS. For example, the ECO at Langley AFB (an Air Combat Command base) reports assets belonging to an on-base field activity of AETC by inserting the code "OJ" into the IPMS MAC field for each affected system or inventory record. This indicates AETC is the MAJCOM owning the equipment.

25.1.3. The MECO, applicable ECO, or the PMO will establish accountability records and reports for system assets obtained. The MECO, applicable ECO, and PMO will enter into an agreement (i.e., memorandum of understanding [MOU], MOA, etc.) that states which individual will enter the information into the IPMS data base. Enter assets when received and update the IPMS to reflect transfer of the assets from the acquiring program office to the Air Force.

25.1.4. Source Documents. Source documents consist of local inventory records, applicable computer systems vendor contracts, and other appropriate local documentation.

26. Transferring Non-Excess Computer Systems Assets to Another Department of Defense Component, Federal Agency, State, or Local Government. The transfer of non-excess computer systems

assets occurs when a function, and the computer systems acquired to support that function, are transferred to another DoD component, federal agency, state, or local government.

26.1. The commanders will execute a MOA between the giving and receiving organizations if an organization outside the Air Force receives computer systems assets, either physically or administratively. The MOA establishes the responsibilities, authorities, and ground rules relative to the transfer. The MOA should have annexes for DRA-supported activities. The parties involved should develop a schedule for reducing and transferring small computer systems workload. Update changes to annexes as they occur.

26.2. The Data Automation Plan (DAP). The DAP includes a complete inventory of equipment, work necessary to develop the transfer schedule, and the time needed to support related tasks.

26.3. To develop a computer system task:

26.3.1. Review all contract obligations (especially maintenance) with the giving and receiving organizations. Pay close attention to any contract termination clauses.

26.3.2. Review computer systems release dates. Give adequate notice to the vendor to preclude payment of extra costs.

26.3.3. Coordinate computer systems release dates with other base functions if necessary.

26.3.4. Sanitize equipment according to security regulations and procedures.

26.3.5. Attach the IPMS records or custodian report for the equipment being transferred.

26.3.6. A designated official from the receiving organization and the ECO must sign and date the transfer document prior to the transfer.

26.3.7. Properly inventory, package, warehouse, and secure equipment when storing computer systems before transfer.

26.3.8. The Air Force ECO must ensure IPMS computer systems inventory records reflect this transfer of equipment accountability to the receiving organization.

26.3.9. Review disposition plans for computer systems program documentation, technical data, etc.

26.3.10. Arrange final disposition and phase-down using associated computer supplies, files, etc.

26.3.11. Send the signed MOA and annexes to HQ AFCIC/SYSS.

Section D—Computer System Maintenance (Not Applicable to Non-Air Force Managed Joint Service Systems)

27. General Information. The CSO coordinates and obtains all required computer systems and associated maintenance. The NCC is the base focal point for computer systems maintenance. Users must follow the computer systems maintenance procedures that the applicable CSO establishes through the OCM, ECO, and NCC.

27.1. Working with base and tenant organizations, the CSO reviews maintenance alternatives annually to ensure the base uses the most cost-effective maintenance options. When maintenance is performed, forward AF Form 597 or vendor maintenance form to the NCC. Information on this form provides data to determine the most cost-effective maintenance.

27.2. Normally, the CSO obtains maintenance and logistics support services, including system and component replacements, by contract. The complexity of computer systems requires systematic and efficient maintenance management. Specifically:

27.2.1. Reliable maintenance practices.

27.2.2. Effective quality assurance.

27.2.3. Close coordination between the applicable CSO, supporting contracting officer, and the contractor.

27.3. The applicable CSO normally coordinates the maintenance of end-user computer systems and components for base and tenant units when they use contract maintenance.

27.4. Tenant organizations provide funding for maintenance of their equipment according to host-tenant support agreements or systems support documents (for standard systems). The applicable CSO coordinates funding with the host budget and accounting and finance offices. NCC controls and tracks maintenance and serves as the contracting officer's technical representative. Contact the applicable CSO or the focal point for guidance.

27.5. Maintenance Contracts. The CSO pursues a consolidated, base-wide maintenance contract with local vendors or maintenance firms as the preferred method when using contract maintenance. If these sources cannot provide cost-effective and responsive support, the CSO uses Air Force-wide contracts or General Services Administration (GSA) non-mandatory schedules. Contracts must provide instructions on how to complete AF Form 597 and vendor forms (if used).

27.5.1. The CSO obtains per-call contractor support, mail-in service, and standby spares rather than on-call support, unless mission requirements dictate otherwise, or a more economic form of support exists.

27.5.2. The CSO must consider combining maintenance support with other nearby government installations to take advantage of possible savings.

27.5.3. The NCC validates needs before ordering contractor maintenance on computer systems. The NCC will determine warranty status of equipment to ensure contract maintenance funds are not used to repair equipment already under warranty. A system-level contract normally covers computer systems that serve as mainframe terminals (such as Phase IV for the standard base-level system). Refer to AFSSI 5102, *Computer Security (COMPUSEC) for Operational Systems*, and the AFSSI and AFSSM 5000-series publications (see AFIND 5) for guidance on managing maintenance contracts for systems that process classified information.

27.6. Computer Systems Maintenance. Maintenance by organizations using computer systems. The OCM or knowledgeable users normally do preventive maintenance on end-user computer systems, unless an organization makes special arrangements. Computer systems managers or users may replace CPUs, keyboards, printers, monitors, and other LRUs if the lease, purchase, or maintenance contracts allow.

27.7. Hardware Maintenance. Organizations that wish to do hardware maintenance below the LRU level must first get approval from HQ USAF/ILM through the CSO and parent MAJCOM. Requests must clearly state why contractor maintenance cannot meet requirements and include:

27.7.1. The cost of tools.

27.7.2. Test and support equipment.

27.7.3. Repair parts stock.

27.7.4. Facilities needed.

27.7.5. Training needed.

27.7.6. Personnel needed.

27.8. Maintenance Procedures. Each MAJCOM director of communications and information, or equivalent, will specify procedures for logging, documenting, collecting, processing, and filing copies of maintenance records in accordance with AFI 37-100 series publications (will convert to AFI 33-300 series).

27.9. Maintenance Policies and Reports. The CSO will review computer systems maintenance policies and maintenance reports at least once a year to determine if service remains responsive to mission needs at the lowest cost.

27.10. Maintenance Coordination. The CSO coordinates maintenance with the command supporting a deployed location before deploying computer systems. Where feasible, the CSO uses contract maintenance while sharing host command or deployed base assets. The CSO may authorize deployment of spare systems or spares kits containing CPUs, keyboards, monitors, printers, disk drives, LRUs, along with support personnel. When HQ USAF/ILM approves maintenance below the LRU level, the CSO considers deploying tools, test equipment, spare components, diagnostic software, and personnel to maintain the computer systems. The CSO should evaluate these costs when planning for deployment maintenance.

28. Emission Security-Certified Maintenance. Due to the high cost of maintaining EMSEC-certified equipment, use EMSEC-certified equipment and maintain EMSEC-certified certification only when you must use EMSEC-certified equipment to achieve the required level of protection. Contact the wing EMSEC officer for further guidance (see AFI 33-203, *The Air Force Emission Security Program*).

28.1. Special maintenance procedures are necessary when using EMSEC-certified equipment. Maintain EMSEC-certified computer systems by using:

28.1.1. Certified contractors (including GSA employees and contractors).

28.1.2. Air Force personnel the vendor has trained and certified (see AFI 21-109, *Communications Security [COMSEC] Equipment Maintenance and Maintenance Training*; AFI 33-203; and AFSSM 7011, *The Emission Security Countermeasures Review*).

28.2. Use alternative maintenance solutions for EMSEC-certified computer systems operating in an environment where changes in national security policy no longer require EMSEC-certified equipment. (**NOTE:** Re-certify computer systems before re-utilization as EMSEC-certified equipment.)

28.3. Contact your wing IP office for guidance before performing or requesting maintenance.

28.4. Contact the CSO or wing IP to arrange re-certification of computer systems before use in an EMSEC environment.

29. Computer Systems Maintenance Reporting. Users will document all computer systems maintenance on AF Form 597 or vendor maintenance forms as specified in the appropriate contract. When ven-

dor forms are not available, or when a specific contract requires them, users will prepare AF Form 597 and provide a copy to the vendor. Each MAJCOM director of communications and information will specify procedures for logging, documenting, collecting, processing, and filing copies of maintenance records in accordance with AFI 37-100 series publications (will convert to AFI 33-300 series publications).

30. Contractor or Air Force Liaison. For Air Force-wide managed systems:

30.1. The responsible CSO refers unresolved maintenance problems between the CSO, the contracting office, and the local contractor representative to the MAJCOM. In addition to working with the contractor's command representative, MAJCOMs (in coordination with the MAJCOM director of contracting) may contact the contractor's corporate level executives. Interested parties should advise HQ AFCIC/SYS if they do not get satisfactory results.

30.2. The NCC coordinates a MOA (or other applicable agreement) with the responsible program manager (PM). The MOA must ensure adequate procedures are in place to obtain and document computer systems maintenance on non-Air Force managed joint service systems.

31. Contractual Matters. The NCC or systems manager must make sure management understands contract terms and conditions to best serve the interests of the Air Force. Each contract should identify when the government earns credits for inoperable equipment. The NCC initiates a claim for credits under the standards of the contract. Support credit claims with a fully documented AF Form 597.

32. Computation of Payments. Contracts applying to managed computer systems.

32.1. Effective Start Date for Rental. The effective date for leased computer systems is usually the first day of the successful acceptance test. A government-caused acceptance test delay may require payment for the delayed period. Consult the individual computer systems contract for specific guidance.

32.2. Computing Charges. ECOs will compute charges for leased computer systems, using the reverse side of AF Form 597, and forward to their MAJCOM for further processing.

32.3. Validating Services. For Air Force-managed systems, the verifying activity refers to the equipment utilization reports and the input to the reports (computer systems/equipment orders, AF Form 597, and other appropriate records), to validate the services. Submit claims for credit within 60 days (or as stated in the contract). The computer systems contract manager designates the verifying activity for non-Air Force managed systems (e.g., joint service systems).

Section E—Disposition of Excess Resources

33. Excess Hardware. The EC notifies the ECO when computer systems become excess to the requirement for which they were initially approved and acquired. However, ECs may retain equipment reported excess as long as there is a valid requirement for it in the using unit. ECOs will decide if they can redistribute the complete system or system components (end items) within the DRA to satisfy validated requirements. Provide this notification at least 120 days before the equipment goes off-line to allow completion of the screening cycle while the equipment is still in use, and eliminate the need to store excess equipment. Until receipt of final disposition instructions, the using organization EC will store the equipment to prevent damage, deterioration, or unauthorized cannibalization. Consider the following:

33.1. When items accounted for in the IPMS become excess to a particular DRA, the ECO creates an electronic excess report in the IPMS using the reutilization module.

33.2. ECOs will use the base or MAJCOM special reporting procedures before releasing equipment for screening at the next higher level.

33.3. The MAJCOM redistribution focal point reviews all finalized electronic excess reports in the IPMS for potential reuse. The MAJCOM has the authority to reuse excess equipment within their command as needs dictate. MAJCOMs also have the authority to transfer excess equipment between commands as required. The Air Force Computer Systems Redistribution Office will resolve conflicts between commands requesting the same equipment.

33.4. The Air Force Redistribution Program Manager will release excess equipment not required within the Air Force to DISA for DoD-wide screening.

33.5. The EC notifies base supply of all excess computer systems equipment accountable for in the base supply system.

33.6. The ECO will notify the OPR when equipment is excess and when to adjust the maintenance contracts. Whenever possible, provide notice 60 days prior to the equipment going off line.

33.7. Outside the continental United States (OCONUS) the ECO approves excess government-owned computer systems (costing less than \$1 million) for turn in to the DRMO.

33.8. The ECO may approve turn in to DRMO of excess government-owned computer systems in unserviceable or scrap condition, except when the equipment is designated for donation to a school under authority of Presidential Executive Orders. Report excess equipment intended for school donation through the IPMS for DoD-wide screening.

33.9. Cannibalization for Spare Parts. The CSO may retain limited amounts of serviceable computer systems for maintenance redundancy and operational spares when the communications unit has a maintenance or operational support mission. He may also approve the cannibalization of unserviceable computer systems hardware as a source of spare parts to maintain other equipment. Only use this authority when a cost analysis clearly determines that it is economically feasible to use excess assets instead of procuring new items. The IPMS will track accountability of complete items retained for maintenance redundancy and operational spares. The ECO cannot serve as the EC for this account. Maintain records for accountability and audit purposes for spare parts cannibalized from unserviceable items.

33.10. Excess Supplies. Report excess expendable computer system supplies to base supply.

34. Obtaining Excess Resources. Use previously declared excess equipment to satisfy approved computer systems requirements when possible. ECOs will review redistribution programs for excess resources to determine if suitable resources are available to satisfy new requirements.

34.1. The IPMS contains information on excess hardware throughout the Air Force. Contact the releasing activity to verify the suitability of the excess before requisitioning. The ECO contacts the Air Force Computer Systems Redistribution Program Office to place a "hold" on excess hardware or software with a DoD case number. The ECO prepares the DD Form 1149 according to the instructions contained in ASD Memorandum dated September 8, 1994, and forwards the DD Form 1149 through command channels.

34.2. The ECO submits requisitions (DD Form 1149) for equipment from DRMO (through the Air Force Redistribution Program Manager) to DISA for approval. The DRMO may release computer systems equipment after receiving approval from DISA.

34.3. ECOs will manage accountability in the IPMS for computer systems equipment acquired through any source.

35. Shipping and Disposition of Excess Computer Systems Resources. Users of computer systems reported excess will retain the equipment to satisfy an operational requirement even if that is after completion of DoD-wide screening or after receipt of an approved requisition. Notify the requester of any delays in the shipment of the equipment. The ECO will promptly ship excess hardware upon receipt of an approved DD Form 1149; Standard Form (SF) 122, **Transfer Order Excess Personal Property**; SF 123, **Transfer Order Surplus Personal Property**; or electronic message from the PM. ECOs will notify the requesting activity to inform them the transfer received approval and to make arrangements for picking up or shipping the equipment. Ship equipment that has completed the screening cycle to DRMO in a timely and economic manner.

36. General Ledger Subsidiary Account-16104. GLSA 16104 accounts for the cost of Air Force computer systems. The GLSA 16104 also includes the cost of government-owned accessories the Air Force did not procure through the supply system. HQ SSG/ENEI provides central reporting of the GLSA 16104 according to Air Force Regulation (AFR) 177-106, *Materiel and Property Accounting*, (will convert to DFAS-DE7420.1-R), with the actual cost of all accountable government-owned computer systems in the Air Force IPMS inventory. Based on current capitalization criteria, HQ SSG/ENEI provides the report in letter format to DFAS/LI-ARF.

37. Checklists. Use the questions at **Attachment 3**, along with AF Form 2519, **All Purpose Checklist** (available electronically), to develop a checklist on computer systems management.

38. Forms Prescribed. This instruction prescribes AF Form 597, **ADPE Maintenance Record**; AF Form 992, **ADPE Identification**; and GSA Form 2068A, **Quarterly Report of ADP Service Provided to Another Agency or Obtained From a Commercial Source**.

WILLIAM J. DONAHUE, LT GEN, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES, ACRONYMS, ABBREVIATIONS, AND TERMS

References

Public Law 104-52, *Telephone Installation and Charges* (31 U.S.C. 1348)

Federal Personnel Manual System, FPM Letter 368-1 dated 26 March 1991, Subject: *Federal Flexible Workplace Project*

ASD Memorandum dated 8 September 1994, Subject: *Interim Management Guidance on Defense Automation Resource Management*

Defense Resource Management Manual, September 1988

DODM5200.28, *ADP Security Manual*, January 1973, with Change 1

AFCAT 36-2223, *USAF Formal Schools*

AFI 21-109, *Communications Security (COMSEC) Equipment Maintenance and Maintenance Training*

AFI 23-111, *Management of Government Property in Possession of the Air Force*

AFI 31-601, *Industrial Security Program Management*

AFI 33-102, *Command, Control, Communications, Computers, and Intelligence (C4I) Capabilities Planning Process*

AFI 33-103, *Requirements Development and Processing*

AFI 33-104, *Base-Level Planning and Implementation*

AFI 33-114, *Software Management*

AFI 33-115, *Networks Management*

AFI 33-203, *The Air Force Emission Security Program*

AFI 64-108, *Service Contracts*

AFIND 5, *Numerical Index of Specialized Information Protection Publications*

AFPD 10-6, *Mission Needs and Operational Requirements*

AFPD 23-1, *Requirements and Stockage of Materiel*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFPD 33-2, *Information Protection*

AFR 177-106, *Materiel and Property Accounting* (will convert to DFAS-DE7420.1-R)

AFSSI 5102, *Computer Security (COMPUSEC) for Operational Systems*

AFSSM 7011, *The Emission Security Countermeasures Review*

Abbreviations and Acronyms

ADPE—Automated Data Processing Equipment

AF—Air Force (*used on forms only*)
AFCAT—Air Force Catalog
AFCIC—Air Force Communications and Information Center
AFGOMO—Air Force General Officer Matters Office
AFI—Air Force Instruction
AFIND—Air Force Index
AFPCA—Air Force Pentagon Communications Agency
AFPD—Air Force Policy Directive
AFR—Air Force Regulation
AFSSI—Air Force Systems Security Instruction
AFSSM—Air Force Systems Security Memorandum
AFTMS—Air Force Training Management System
AIS—Automated Information System
ANG—Air National Guard
ANGIND—Air National Guard Index
ARMS—Automation Resources Management System
ASD—Assistant Secretary of Defense
CPU—Central Processing Unit
CSM—Computer Systems Management
CSMWG—Computer System Management Working Group
CSO—Communications and Information Systems Officer
CSSO—Computer Systems Security Officer
DAA—Designated Approving Authority
DAP—Data Automation Plan
DAR—Data Automation Requirement
DD—Department of Defense (*used on forms only*)
DDN—Defense Data Network
DFAS—Defense Finance and Accounting Service
DISA—Defense Information Systems Agency
DISN—Defense Information Systems Network
DoD—Department of Defense
DRA—Defense Reporting Activity Account

DRMO—Defense Reutilization and Marketing Office
EC—Equipment Custodian
ECO—Equipment Control Officer
EMSEC—Emission Security
FOB—Found-On-Base
FPI—Functional Process Improvement
GLSA—General Ledger Subsidiary Account
GO—General Officer
GSA—General Services Administration
HQ AETC—Headquarters Air Education and Training Command
HQ AFCA—Headquarters Air Force Communications Agency
HQ SSG—Headquarters Standard Systems Group
HQ USAF—Headquarters United States Air Force
IMPAC—International Merchant Purchase Authorization Card
IP—Information Protection
IPMS—Information Processing Management System
IRCEN—Interagency Report Control Number
LAN—Local Area Network
LRU—Line Replaceable Unit
MAC—Major Command Code
MAJCOM—Major Command
MECO—MAJCOM Equipment Control Officer
MOA—Memorandum of Agreement
MOU—Memorandum of Understanding
NCC—Network Control Center
NIPRNET—Non-Classified Internet Protocol Network
OCM—Organization Computer Manager
OCONUS—Outside the Continental United States
OPR—Office of Primary Responsibility
PC—Personal Computer
PCS—Permanent Change of Station
PM—Program Manager

PMO—Program Management Office
POM—Program Objective Memorandum
ROS—Report of Survey
SA—Systems Administrator
SCIF—Sensitive Compartmented Information Facility
SE—Senior Executive
SES—Senior Executive Service
SF—Standard Form
UTC—Unit Type Code

Terms

Air Force Infrastructure Support Contracts—Contracts that provide small computer resources at discount prices, and a standard structure for Air Force-wide interoperability with other small computers (formerly known as Air Force computer requirements Contracts, Indefinite Delivery/Indefinite Quantity, and Requirements Contracts)

Cannibalization—The act of removing serviceable parts from one computer system for installation in another computer system when removal of parts will cause the first system to not perform as designed.

Central Processing Unit (CPU)—The portion of a computer that executes programmed instructions, performs arithmetic and logic functions, and controls input and output functions. One CPU may have more than one processor housed in the unit.

Command, Control, Communications, and Computer (C4) System—An integrated system of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control, through all phases of the operational continuum. This system includes visual information support systems. Within the Air Force referred to as Communications and Information systems.

Communications and Information Systems Officer (CSO)—The term CSO identifies the supporting systems officer at all levels. At base level, this is the commander of the communications unit responsible for carrying out base Comm and Info systems responsibilities. At MAJCOM, and other activities responsible for large quantities of Comm and Info systems, it is the person designated by the commander as responsible for overall management of systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol SC that is expanded to three and four digits to identify specific functional areas. CSOs are the accountable officer for all automated data processing equipment in their inventory.

Computer System—A functional unit, consisting of one or more computers and associated software, that (a) uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program; (b) executes user-written or user-designated programs; and (c) performs user-designated data manipulation, including arithmetic and logic operations. **NOTE:** A computer system may be a stand-alone system or may consist of several interconnected systems. Personal computers, microcomputers, minicomputers, multi-user systems, all standard multi-user small computer requirements contract systems, text processors, word processors, intelligent typewriters, workstations, are

examples of computer systems.

Department of Defense (DoD) Redistribution Program—Worldwide program, initiated by DoD for reporting, screening, redistributing, and disposing of automation resources that have become excess under an original application.

Designated Approving Authority (DAA)—The organization or individual that establishes necessary procedures and controls to protect information and ensures the availability and integrity of critical processes. Refer to AFSSI and AFSSM 5000-series publications for additional information.

Documentation—The formal standardized recording of detailed objectives, policies, and procedures governing conception, authorization, design, testing, implementation, operation, maintenance, modification, and disposition of data administration techniques and applications. All DoD computer systems documentation is written in accordance with DOD Instruction 7935.1-2.

Emission Security (EMSEC)—Short name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

Equipment Control Officer (ECO)—An individual appointed by the applicable communications-information systems officer to manage and control computer systems resources for a base. (NOTE: MAJCOMs may appoint a tenant ECO to provide computer systems control and accountability for their tenant units.)

Equipment Custodian (EC)—An individual who acts as a subordinate to the equipment control officer (ECO) and performs inventory, utilization, and maintenance recording and reporting and other custodial duties as the ECO requires.

Hardware—1. The generic term dealing with physical items as distinguished from its capability or function such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, and parts. The term is often used in regard to the stage of development, as in the passage of a device or component from the design stage into the hardware stage as the finished object. 2. In data automation, the physical equipment or devices forming a computer and peripheral components. See also software.

Joint Service System—A standard system implemented at one or more services sites (U.S. Army, U.S. Navy, U.S. Air Force, and U.S. Marine Corps). System acquisition, development, maintenance, and life-cycle support are assigned to a program manager assigned to one of the services.

Life-Cycle Management—1. The management of a system or item, starting with the planning process and continuing through successive management processes and associated life-cycle management phases and associated milestones, until a system is terminated. 2. A management process, applied throughout the life of an automated information system (AIS), that bases all programmatic decisions on the anticipated mission-related and economic benefits derived over the life of the AIS.

Line Replaceable Unit (LRU)—A module, subassembly, or printed circuit card you can replace or repair without soldering.

Maintenance—1. All action taken to retain materiel in or to restore it to a specified condition. It includes: inspection, testing, servicing, classification as to serviceability, repair, rebuilding, and reclamation. 2. All supply and repair action taken to keep a force in condition to carry out its mission. 3. The routine recurring work required to keep a facility (plant, building, structure, ground facility, utility system, or other real property) in such condition that it may be continuously utilized, at its original or

designed capacity and efficiency, for its intended purpose. 4. The function of keeping (C4) items of equipment in, or restoring them to, serviceable condition. Maintenance is not intended to increase the value, capabilities, or expected life of a system. Equipment maintenance includes servicing, repair, modification, modernization, overhaul, inspection, condition determination, corrosion control, and initial provisioning of support items. Maintenance includes both preventive and corrective actions. Software maintenance includes anticipating, detecting, and eliminating errors.

Major Command Equipment Control Officer (MECO)—The individual appointed by the major command (MAJCOM) communications and information systems officer to manage and control computer systems resources for a MAJCOM.

Network Control Center (NCC)—The base focal point for network management, problem resolution and, computer maintenance issues (formerly known as Base Network Control Center [BNCC]).

Peripheral—Any equipment that provides the computer with additional capabilities distinct from the central processing unit. Examples are a printer, mouse, disk drive, digitizer, etc.

Protocol—In data communications, (a) a set of rules governing network functionality. The open system interconnection reference model uses sets of communication protocols to facilitate communications between computer networks and their components, or (b) a formally specified set of conventions governing the format and control of inputs and outputs between two communicating systems.

Resources—Any computer system, computer system component hardware and software, contractual services, personnel, supplies, and funds.

Shareware—Privately or commercially developed software that is normally distributed free of charge but a fee is generally expected for continued or extended use. Normally, implied or promised support by the author is minimal or nonexistent.

Software—1. A set of computer systems programs, procedures, and associated documentation concerned with the operation of a computer system (i.e., compilers, library routines, manuals, circuit diagrams). 2. The programs, procedures, rules, and any associated documentation pertaining to the operation of data processing systems.

System—A computer system and its external peripherals and software interconnected with another computer system. Typical “systems” include laptop personal computer (PC), desktop PCs, networked and distributed computer systems (e.g., servers, workstations, data management processors, etc.), mainframe and “midsize” computers and associated peripherals.

Systems Administrator—The organization focal point for multiuser systems.

Wing Information Protection (IP) Office—Office that administers the wing IP program, advises the base computer systems security officer, and acts as the accreditation advisor to the designated approving authority. The office is within the wing communications unit.

Attachment 2

KEY ORGANIZATIONS

Defense Finance and Accounting Service (DFAS/LI-ARF)

3 Arkansas Road

Limestone ME 04751-1500

HQ Air Force Computer Systems Redistribution Program Office (HQ AFCIC/SYSS)

1250 Air Force Pentagon

Washington DC 20330-1250

DSN: 227-5897/Fax: 224-7998

HQ Air Force Communications Agency (HQ AFCA/XPPD)

203 West Losey Street, Room 1065

Scott AFB IL 62225-5224

DSN: 576-5475/Fax: 576-2874

HQ Air Force Communications Agency (HQ AFCA/SYND)

203 West Losey Street, Room 3065

Scott AFB IL 62225-5234

DSN: 576-8771/Fax: 576-8682

Air Force General Officer Matters Office (AFGOMO)

1040 Air Force Pentagon

Washington DC 20330-5292

DSN: 224-6184/Fax: 227-5292

Air Force Pentagon Communications Agency (AFPCA/LASA)

ATTN: DRA (DPI) 3500

1400 S. Eads Street

Arlington VA 22202-9881

DSN: 332-9881/Fax: 332-8034

Air Force Technology Verification Office (OL-B, HQ AFCA/TN)

245 Davis Avenue East, Room 2

Barksdale AFB LA 71110-2278

DSN: 781-2756/Fax: 781-2638

HQ USAF/ILM

1030 Air Force Pentagon

Washington DC 20330-1030

DSN: 223-7756/Fax: 225-9811

HQ USAF/SCXX

1250 Air Force Pentagon

Washington DC 20330-1250

DSN: 227-3150/Fax: 227-2100

Desktop III/IV/V Program Office

HQ Standard Systems Group (HQ SSG/SSM)

85 Hodges Avenue South, Building 403

Maxwell AFB-Gunter Annex AL 36114-3218

DSN: 596-3282/Fax: 596-3262

Air Force Communications and Information Center (HQ AFCIC/ITC)

Records Management

1250 Air Force Pentagon

Washington DC 20330-1610

DSN: 224-4263

HQ Standard Systems Group (HQ SSG/XPT)

Documentation Standards

200 East Moore Drive, Building 888

Maxwell AFB-Gunter Annex AL 36114-3004

DSN: 596-4843/Fax: 596-4668

HQ Standard Systems Group (HQ SSG/SSMC)
85 Hodges Avenue South
Maxwell AFB-Gunter Annex AL 36114-3218
DSN: 596-3671/Fax: 596-3262

HQ Standard Systems Group (HQ SSG/ENEI)
102 Hodges Avenue South
Maxwell AFB-Gunter Annex AL 36114-3220

HQ Standard Systems Group (SSG/SSMCM)
SMSCRC Program Office
ULANA Operating System Software Contract
85 Hodges Avenue South
Maxwell AFB-Gunter Annex AL 36114-3218

Attachment 3

QUESTIONS FOR COMPUTER SYSTEMS CHECKLIST

- ____ 1. Has a memorandum of agreement (MOA) been established for addressing responsibilities for deployment and support for joint systems?
- ____ 2. Has an equipment control officer (ECO) been appointed (in writing) by the commander?
 - ____ a. Has the selected individual received appropriate training?
 - ____ b. Does the selected individual meet the criteria as noted in paragraph 10?
- ____ 3. Has the commander delegated the authority to receive new equipment to only the ECO?
- ____ 4. Has the applicable ECO received certification that equipment custodians (EC) have completed their annual inventory?
- ____ 5. Has an EC been appointed, in writing?
- ____ 6. Are Reports of Survey being accomplished in a timely manner?
- ____ 7. Do departing ECs process out through the ECO?
- ____ 8. Has a joint inventory been accomplished by BOTH incoming/departing ECOs?
- ____ 9. Has a joint physical inventory been accomplished prior to equipment account transfer?
- ____ 10. Have command supplements been coordinated through HQ AFCA/SYND?
- ____ 11. Have EC changes been reported to the base or tenant ECO not later than 30 days before the change?
- ____ 12. Have accountability records been established for system assets acquired through a joint service program office?